CHAPTER 6

Cyber Ranges: The New Training Era in the Cybersecurity and Digital Forensics World

Athanasios Grigoriadis, Eleni Darra, Dimitrios Kavallieros, Evangelos Chaskos, Nicholas Kolokotronis, and Xavier Bellekens

6.1 Introduction

Nowadays, cybersecurity is considered as the key factor that an organization can be affected by a security incident. As there is a huge growth of cyber-attacks, successfully thwarting cybersecurity threats has become crucial up to the level of protecting people's everyday lives and the effect they

A. Grigoriadis (✉) · E. Darra
Center for Security Studies, Athens, Greece
e-mail: a.grigoriadis@kemea-research.gr; e.darra@kemea-research.gr

D. Kavallieros
Center for Security Studies, Athens, Greece

University of Peloponnese, Tripoli, Greece
e-mail: d.kavallieros@kemea-research.gr; d.kavallieros@uop.gr

B. Akhgar et al. (eds.), *Technology Development for Security Practitioners*, Security Informatics and Law Enforcement,
https://doi.org/10.1007/978-3-030-69460-9_6

may have on a large number of businesses every year. For this reason, cybersecurity training can play a vital role in avoiding and defending against cyber-attacks and for securing systems, networks, and data, since they will teach all businesses' stuff involved how to protect against cybersecurity threats. Additionally, a cyber range (CR) is a micro-environment that offers tools and services to support the establishment of cybersecurity training courses and cybersecurity exercises to enhance the resilience and increase of cybersecurity capabilities of organizations. Furthermore, a cyber range allows the reproduction and execution of information technology (IT), operational technology (OT), and/or hybrid systems in a real or simulated environment. The diversity of cyber ranges across different sectors leads to the imperative need to review their current status focusing on the infrastructure they utilize and other relevant approaches having been taken into account for their development.

In this chapter, 27 CR environments are presented in Sect. 6.2, giving a short description of their capabilities, mission, and configuration features they embed and, in some cases, the highlighted advantages. The IT, OT, and Hybrid approaches of the CRs are presented in Sect. 6.3. Section 6.4 provides a full overview of the components of CRs, whereas Sect. 6.5 presents the operational impact of cyber ranges elements. The example of FORESIGHT approach, which brings together the state-of-the-art features of cyber ranges, is given in Sect. 6.6. Finally, a summary of this chapter is presented.

6.2 State-of-the-Art of Cyber Ranges

A CR can be categorized by the supporting sector, such as government (incl. military and LEAs oriented), academic, and commercial; its development depends on the design of several features such as flexibility, scalability, isolation, interoperability, effectiveness, access, service-based access, scoring and evaluation, and risk evaluation.

E. Chaskos · N. Kolokotronis
University of Peloponnese, Tripoli, Greece
e-mail: e.chaskos@uop.gr; nkolok@uop.gr

X. Bellekens
University of Strathclyde, Glasgow, UK
e-mail: xavier.bellekens@strath.ac.uk

6.2.1 Government, Military, and LEAs Oriented

It is well defined in the literature that there are plenty of CRs that have been indicated and identified in the government and military organizations determining the importance of cybersecurity training. Below some of the most known and often used cyber ranges for government and military organizations are presented.

6.2.1.1 Department of Defence (DoD) Cybersecurity Range

DoD CR environment is capable to support exercises, training, testing, evaluation, and education especially for the military parts [1]. Some of the modules embedded in this CR are the traffic generator, configurable user emulation, malware, spyware, and botnets emulation.

6.2.1.2 Arizona Cyber Warfare Range

The Arizona Cyber Warfare Range is a live-fire cyber warfare range created to rapidly train/upskill cybersecurity talent with hands-on learning [2]. Cyber Warfare Range drives innovation in cybersecurity techniques, technologies, and training across the United States and allied countries. This range is a privately funded non-profit entity and is 100% volunteer-driven.

6.2.1.3 Hybrid Network Simulation (HNS) Platform

HNS platform is an all-in-one cyber range that makes use of a turnkey platform for technical and operational preparedness of civilian and military cyber defenders. It includes multiple operations like up-to-date cyber range features and scenarios and a hyper-realistic and dedicated environment outside production systems for training in a red-blue team environment [3].

6.2.1.4 ManTech

ManTech is built on as an Infrastructure-as-a-Service model, coupled with more than a dozen tools. It instantly provides a precise emulation of any network environment, regardless of size, at any level of fidelity. Users have the ability to create replicas of existing systems and network structures and then to simulate those environments with realistic traffic, automated users, and even malware [4].

6.2.1.5 École Navale CR

École Navale's CR environment is used to support training and education for students, military, and researchers. It mainly focuses on naval systems, supervisory control and data acquisition (SCADA), and navigation equipment and makes use of the same programmable logic controllers (PLC) which are used on real ships. Furthermore, it is very flexible with virtual capacities. It is worth mentioning that services are still under construction [5].

6.2.1.6 Airbus CR

Airbus CR environment may support training and education for companies and the military. Specifically, it includes complete training stack, trainer console, training scenarios advanced customization tools, malware forensics, network security, penetration testing, certification, capture-the-flag benefits, user-friendly interfaces, and simplified management of the virtual environment. Some of the most worth-mentioned services are live traffic generation, individual and team training, multistep scenarios of threat, quick design and deployment of network infrastructures through a user-friendly interface, and customizable catalogue of assets and cyber-attacks [6].

6.2.2 Academic

There have been several efforts from universities to simulate the effects of computer network attacks. These approaches are primarily used for training and research from the students. An extensive list and description of the CRs are described below as follows.

6.2.2.1 KYPO Cyber Range

This CR is a realistic environment for cyber-training and support for cyber-testing, research, and training for students and researchers [7]. As hosted in the cloud, it includes several capabilities of web access, role-based access, user-specific content, dynamically creation and destruction of the virtual environments, and large target network replication for multiple and simultaneous usages. Some of the most important features include the complete training stack, training scenarios, advanced customization tools, malware forensics, network security, penetration testing, certification, and the benefit of capture-the-flag (CTF) environment.

6.2.2.2 Augusta University CR

The Augusta University CR environment is able to support exercises and training for education and research [8]. It is a training methodology that can lead to certified courses keeping in.

6.2.2.3 US Cyber Range

US CR is a scalable, cloud-hosted infrastructure that provides users with a virtual environment for realistic, hands-on cybersecurity labs and exercises [9]. One of the key features of this CR is that it is defined as an immersive environment because students can practice what they've learned in hands-on laboratory exercises. Furthermore, it is a cloud-hosted infrastructure that can be accessed from any device either from school or home, and instructors can deploy cloud-based virtual environments to students using a simple point-and-click interface. Additionally, having administrative access to the instance of cyber range software, customers create accounts for faculty and other cyber range users.

6.2.2.4 Austrian Institute of Technology Cyber Range

The Austrian Institute of Technology's CR is an environment for sharing knowledge in the cybersecurity domain for critical infrastructure providers, industry, research, and the public sector [10]. Advanced training exercises and competition on different levels, visualization, industrial control systems, digital networks, and critical infrastructures focus on cybersecurity research and development.

6.2.2.5 Saros Technology

Saros CR uses manufacturers like Cisco and Ixia's virtual machines to create real infrastructure for developing real cyberthreat scenarios [11]. Fully virtualized, the Virtual Test Lab is available on-demand, reusable, easily replicated, and self-service. Each cloud is executed as its own single file and is treated just like a document so it can be edited, copied, shared, and backed up.

6.2.2.6 European Space Agency (ESA) CR (by RHEA Group)

This CR is focused on cybersecurity and computer network defence for ESA [12]. The embedded services are instantiation of a full mission environment, mission control systems, pre-launch, launch, IoT, ground and satellite simulators, and operations and development network. It claims to be the perfect environment to support training and education.

6.2.2.7 Virginia CR

This CR provides an environment to increase the number, and the preparedness, of students entering the cybersecurity workforce in operations hosted in the cloud, web access, role-based access, user-specific content, dynamic creation and destruction of the virtual environments, and large target networks which can be replicated for multiple and simultaneous usages [13].

6.2.2.8 THE Michigan CR

The Michigan CR aims to strengthen Michigan's cyber defences by mitigating the growing number of cyberthreats and providing a more secure environment that promotes economic development. This can be accomplished by nurturing a cybersecurity industry that leverages Michigan's unique advantages, which include educational institutions, a large IT workforce, the manufacturing base, and federal cooperation with the security industry [14].

6.2.3 Commercial

Several commercial cybersecurity simulation products exist in the market. In the list below, there are the general-purpose CRs, without a specific academic or military orientation but with the possibility to be used by multi-domain users.

6.2.3.1 IXIA Cyber Range

This CR is used to provide an environment to train the participants of an organization to combat modern cyberthreats using a variety of IXIA's products. It can offer a service, flexible, scalable, application and threat intelligence, visualization modules, security information and event management (SIEM), and traffic generator. It can also provide complete training stack, trainer console, training scenarios, advanced customization tools, various training scenarios, capture-the-flag environment, and cybersecurity competitions [15].

6.2.3.2 Palo Alto Networks Cyber Range

It is used to train the participants of an organization to combat modern cyberthreats and enhance their prevention, detection, and response skills through hyper-realistic network simulation exercises [16]. It can also provide an isolated and realistic environment with network traffic-generator

capabilities, application traffic-generator, and the support of multiple courses.

6.2.3.3 IBM Cyber Range

IBM CR delivers an environment in order to offer a training experience in a cyber-incident [17]. The objective is to exercise a rapid-response thinking in a pressured environment, understand how security solutions work together and experience on how the teams work together.

6.2.3.4 CybExer Cyber Range

CybExer CR is an environment that supports training and education for companies, military, and LEAs [18]. It offers a complete training stack, trainer console, training scenarios, advanced customization tools, malware forensics, network security, penetration testing training, certification, and CTF environment.

6.2.3.5 Raytheon Cyber Range

Raytheon CR provides an environment to support training and education for all different companies [19]. It offers a network environment emulation for air traffic control, power grids, water supplies, security operations centre (SOC) capabilities, scalable and agile architecture, automation, and interconnection with external hardware.

6.2.3.6 CYBERBIT Cyber Range

This CR is able to provide a hyper-realistic simulated training environment to enterprises, governments, and academic institutions [20]. This CR prepares the security team for the attack, by providing a complete training stack, trainer console, training scenarios, advanced customization tools, malware forensics, network security, penetration testing, certification courses, and capture-the-flag environment.

6.2.3.7 Breaking Point

Commercial appliances from breaking point are advertised as providing CR capabilities [21]. Their products provide traffic generation and a strike pack of network security and malware attacks in a single rack-mountable appliance. Traffic generation is highly configurable up to and including layer 7 of the Open Systems Interconnection (OSI) model. Breaking point uses simulation to achieve its high scalability. Large network topologies

involving hundreds of thousands of hosts can be simulated in a single appliance.

6.2.3.8 RGCE

The Realistic Global Cyber Environment (RGCE) utilizes modern ways to combine virtualization techniques, physical devices, and business-specific systems [22]. It is also possible to create tailored environments for an organization's specific training, exercise, or research and development needs. RGCE provides individual training for cybersecurity specialists, security analysts, and pen-testing operators, cybersecurity training and capability development for organizations and teams, ready-made business sector organization environments, digital forensics, and incident response training and exercises.

6.2.3.9 Berkatweb

Berkatweb is a cyber range with features with various security challenges and the ability of modelling and simulation of dynamic exercises and a fully customizable API framework [23]. This CR provides an extensible virtualized platform for cybersecurity training, modelling, simulation, and advanced analytics. It offers a secure environment in which to assess network and system attack and defend strategies as well as supplies a proven training path, helping your organization improve its cyber resilience and maturing. The CR's architecture gives users the ability to test, evaluate, and train for next-generation threats, similar to training on a traditional weapons test range.

6.2.3.10 CYBERGYM

CYBERGYM emulates complex cyber-attack scenarios in OT and IT environments [24]. Apart from that, it is a common cyber range model which provides training for all departments, specializing in active cyber defence, event mitigation, and crisis management. The three teams participate in the training sessions including the red team, the blue team, and the white team. Utilizing the red team throughout the training provides unique insights into a hacker's mindset and point of view. The blue team is faced with real attacks they have to identify, defend, and harden their environment against using the necessary methods and tools, while the white team manages the training and debriefing process, reviews the blue team's performance, and provides recommendations.

6.2.3.11 CyberCENTS

The CENTS® platform solutions provide a relevant, integrated, Live-Virtual-Constructive (LVC) cyber range environment for demonstration, training, exercising, tool development, and testing full-spectrum cyberspace capabilities [27]. The CENTS solution permits closed-network engagements or use of a virtual private network (VPN), engagements with multiple interconnected environments. Each CENTS unit has an IEEE RFC-compliant traffic generation that features dynamic traffic flows and protocols that can be manipulated to follow a customer profile. The emulated elements of the environment (e.g. users, traffic, attacks, the Internet) interact with the virtualized and physical elements of the system providing true-life system response. This CR supports social media services and multilayer and dynamic websites. All IP addresses and website URLs resolve in the cyber range's domain name system (DNS). All virtualized Internet IP space uses real-world geo-IP addresses. The cyber scenarios can be executed in automatic or manual mode.

6.2.3.12 Silensec Cyber Range

The key benefit of Silensec CR includes cloud technology improvement on how to scale up to thousands of concurrent users and virtual environments. It is available as a service or hosted as a highly secure on-premise cyber range, capabilities for integration with IoT and supervisory control and data acquisition/industrial control system (SCADA/ICS) environments. Additionally, it supports individual and team-based cyber exercises, not to mention the competence-based scoring and assessment system embedded [28].

6.2.3.13 Cisco Cyber Range

The Cisco Cyber Range is offered as a service [38]. It is a training course that aims to train the participants to combat modern cyberthreats. Cisco CR is based on real-world scenarios and provides a war-gaming environment that allows participants to play the role of both the attacker and the defender, in order to learn the latest methods of vulnerability exploitation and the use of advanced tools and techniques to mitigate the threats. The Cisco CR provides real-life experience of reacting to and defending against complex cyber-attacks, including advanced persistent threats (APTs). It provides training in security methodologies, operations, and procedures using a variety of security tools and techniques.

6.3 IT, OT, and Hybrid Approaches of Cyber Ranges

Cyber ranges offer an environment for teams to train collectively, improve their cyber defence skills, and gain critical insight into a variety of stakeholder actions within every organization. This tends to improve teamwork across the enterprise and the communication skills between stakeholders as it gives teams a better understanding of what other departments or people are responsible for. This is critical to building a successful incident response team, and it's difficult to obtain that experience through conventional training simulations. Teams are trying to support an IT environment, an OT environment, or most often a combination of them, a hybrid one. In the table below, a categorization of CRs is depicted depending on the approach of the network environment and their involved assets:

CR approach	*Description*	*Implementation*
IT	IT cyber ranges provide a complete and tested framework to help IT security organizations improve their overall security posture. Used by companies and governments around the world, cyber ranges offer hyper-realistic simulated training and testing scenarios, which dramatically improve cybersecurity performance while providing tools for simulating various network setups, attack scenarios, and traffic patterns	As network attacks have been very common now, understanding their mechanism and knowing how to detect and respond to it is essential to the cybersecurity of every enterprise. Distributed denial of service (DDoS) SYN flood, DNS amplification attack, and man-in-the-middle attack will be taught in the hacker's perspective and the defender's perspective to equip the students with an all-rounded understanding of the attacks and prevention approaches
OT	Hands-on training simulations that are ultra-realistic and safe regarding that OT services and machines rely on	It is about the creation of a replica environment of an operational ecosystem of an organization in order to exercise on it. That means the hardware and software detect or cause a change through the direct monitoring and/or control of physical devices, processes, and events in the organization. Further to that, it is related to testing, fine-tuning, and perfecting the response to cyber incidents. The result is to gain interactive hands-on learning by leveraging the OT incident response and building an integrated cyber response strategy

CR approach	*Description*	*Implementation*
Hybrid	Traditional IT security training is largely ineffective because it relies on sterile, mostly theoretical training. To get the security teams prepared to face today's multidimensional IT and OT security challenges, the focus should be in a technology-driven environment that mirrors organizations own, facing real-life threats. In other words, it could be defined as hyper-realistic hybrid simulation	The potential of simulation-based training, as compared to traditional training, is substantial. Organizations can not only train people but also test processes and technologies in a safe environment. Furthermore, security teams can be trained as individuals or as a group, to improve their teamwork. With the help of simulation, a team can experience high-fidelity threat scenarios while training and improve their capabilities, rather than encountering these threats for the first time during the actual attack. This results in a dramatic improvement in their performance

6.4 Components of Modern Cyber Ranges

Modern cyber ranges are referring to the ones that need realistic, industry-relevant content as well as trainees' tools to practice governance activities in emulated networks. This will help all trainees to better understand how to address a threat in real-life scenarios. It is well-known that cybersecurity attacks require teams to combat them, and for that reason cyber ranges are able to allow the team training and engagement for professionals to gain a better understanding of what it really needs to be taken into consideration in order to stop evolving threats.

6.4.1 Artificial Intelligence (AI) and Machine Learning

With advances in AI and machine learning, cyber ranges are considered vital to leverage such technologies, especially in the last few years. The collected intelligence from the information gathering component and the collected network-flow samples from various attacks will feed the threat data visualization tools, threat simulation tools, and threat forecasting tools regarding AI and machine learning new capabilities and "zero-day" features. Big data and machine learning can enhance this process by learning how to automatically detect unusual patterns in web traffic. The huge

raise of encrypted traffic makes machine learning valuable because of its capability of monitoring previously unseen encrypted network traffic [25]. Additionally, a threat forecasting module can help to improve the security posture prior to an attack regarding such kind of attacks. The holistic view with the gathered intelligence accompanied by the data analysis of the pattern and trends of the attacks and the network flow analysis of AI and machine learning will improve the cybersecurity awareness of trainees (e.g. LEAs). In the end, they will be able to build a threat modelling for their needs of proactive data-driven by big data analysis [26].

6.4.2 Information Gathering and Sharing

An important element of the planning stage of a cyber range training scenario is to ensure that scenarios are realistic and up to date. In order to achieve this, it is necessary to receive information from multiple sources. such as the process of sharing data on attacks, malware, malware indicators, indicators to compromise, research statistics, incident reports, or even suspicious actions and methodologies. Results and conclusions from threat hunting and research procedures related to the training scenario under development should also be included [29]. Cooperation and information sharing are considered to be a key important training objective during a cyber defence exercise or training in a cyber range as dependencies between each other systems, similar networks, and similar attacks should foster cooperation and information sharing between the blue teams [31]. It should be mentioned that information sharing is also included in the major aspects of special scoring during the evaluation phase. There are various modules and extensions used for threat information sharing framework which are used for collecting, processing, and exporting high-quality indicators of compromise (IOCs). This allows a security analyst or a player – blue team leader to collect and standardize structured and unstructured threat intelligence. Applying threat intelligence to security operations enriches alert data with additional confidence, context, and co-occurrence. This means that users and trainees can apply research from third parties to security event data to identify similar, or identical, indicators of malicious behaviour and enrich a scenario with it.

6.4.3 *Gamification and Serious Gaming*

In the context of training and military strategy, games and simulations are well-known to Roman military commanders as tools to visualize and manipulate small physical representations of battlefields as Smith R. said in [33]. Nowadays, various methodologies have endeavoured to introduce gaming components in cybersecurity education using cyber ranges. These methodologies vary from using simple games for beginners and non-experts to cybersecurity training ecosystems for cybersecurity professionals from the frame of cybersecurity sectors. Through gamification, trainees can obtain the appropriate practical skills and the corresponding to an incident or a special cyber-attack occasion. A problem-solving mechanism through lab environments enables the participants to grasp the problem's full details but also the key decision-makers to find a solution, in a cybersecurity incident, which increases cyber-resilience and their creative-thinking methods. Most of the game genres are applicable to cybersecurity training as well [26].

Serious gaming is simulations that are often adopted by those organizing cyber war games, involving the drilling or training of military and security personnel. These types of games are a cyber version of different activities well-known in the military and/or LEAs. One type of cyber exercise that can utilize a full-scale simulation is an activity known as "capture the flag". CTF activities are often selected for large, international exercises, such as Locked Shields [36]. CTF is a form of war gaming where participants are divided into red and blue teams, with red teams playing the part of the aggressor or hacker and blue teams defending. Depending on the nature of the scenario, blue teams may be required to work together or independently to achieve game goals. In gameplay, teams are awarded points depending on how deep they penetrate a defended network or how swiftly they respond to and remedy an incident or attack.

6.4.4 *Evaluation Module*

The exercise life cycle ends with an evaluation. As cyber range is the testbed for cybersecurity and cyber defence exercises, an evaluation should be conducted after the exercise training in a specific cyber range that consists of a collection of:

- Evaluation (after action) workshop
- Feedback survey (after-action report)
- Scoring subsystem

The most visible part of this phase is the evaluation workshop attended by the blue team (CR defenders' team). The red team (CR attackers' team) prepares an overview of its success in attacks against particular teams and best practices related to the attacks used in the exercise. Both teams benefit from data collected and entered into the scoring subsystem. Furthermore, the green team (CR technical team) stores all collected logs during the exercise of other teams if needed. Feedback provided by the blue teams in the survey before the evaluation workshop is also incorporated. The evaluation workshop shows the exercise scenario and timeline from the perspective of the red team and the white team. It is the only opportunity when the learners can authoritatively learn about attacks used by the red team. They can discuss their approach in particular situations and phases. Until this point, they were only able to see the results of their experimentation during the exercise without an explanation of why something happened. It is therefore recommended not to underestimate this part of the exercise and deliver analysis and lessons that will have value to the learners. For instance, a handout with best practices for system hardening might be useful in the daily routine of the participants [30]. During the evaluation phase, a member of the design team or another selected staff member should develop an after-action report that determines the functionality of the tested systems or components [32]. The introduction to the after-action report should document background information about the test such as the scope, objectives, and tests. The after-action report should also document observations made by the test team during the test and recommendations for enhancing the IT plan that had its components or systems tested, along with associated procedures and components. The after-action report should also include a list of test participants and may provide information from any participant surveys that were distributed during the hotwash (workshop) to solicit feedback.

Not only during the exercise life cycle but especially during the evaluation workshop and the after-action report, evaluation tools should be used. The main tool is a scoring subsystem which is used for the penalization of blue teams' life cycle. During this phase, scenario-specific data is used to define scoring rules. Attack plans, objectives, and penalty values are set according to the expected goals of the exercise and learners' skills

[31]. The scoring system is considered an essential part of CR exercises and provides feedback and the option for comparison to the technical blue teams (BTs). The scoring system is a mixture of graded procedures by human evaluators and an automated process by CR systems. The scoring aspects that can be measured are based on the red team (RT) reporting, analysis of yellow team observations, and decisions of white team members. Detailed scoring rules should not be released to the BTs or players in order to avoid them focusing only on how to get higher scores. The following categories are proposed to be measured [31]:

- Availability of services
- CR usability
- Successful red team attacks
- Situation reporting
- Responding to injects
- Requests for support to GT
- Special scoring

where the last category includes penalties, bonus points for outstanding performance, and information sharing, amongst others.

6.5 Operational Impact of Cyber Range Elements

The advantages of using exercises such as simulations as training tools have been well-known especially to military and security personnel for centuries. Such activities provided practice for soldiers in preparation for real situations and actual combat.

6.5.1 Impact of Training in Cybersecurity/Defence

From the perspective of organizational learning, there is no fundamental difference between a simulated event and a real incident [35]. Conducting cyber range exercises can help with validating policies, plans, and procedures and with training, improving current tools, or rolling out new equipment; testing information and communications technology (ICT); and identifying gaps in resources. As a result, this kind of exercises is of benefit to a broader range of actors and organizers than simply military and security law enforcement organizations [33]. Cyber range training can be carried out by small, individual entities such as single ministries or

private firms or, in the case of large multinational simulations, exercises which can involve a multitude of actors from different areas of the security nexus, such as private corporations, government ministries, utility providers, and military units. Additionally, cyber ranges tend to be highly technical in nature with a focus on testing technological capabilities and resources. This is an important aspect of national cyber defence and cybersecurity in combination with full-scale simulations in procedural scenarios. Conflict in cyberspace, while new and technically challenging, still conforms to traditional models of conflict. As do defenders of other domains, defenders of cyberspace strive to minimize the fog of war (is the uncertainty in situational awareness experienced by participants in military operations), either deliberately or intuitively. However, the volume, velocity, and variety of operations in the cyber defence domain, coupled with enormous attack surfaces and the low cost to adversaries of mounting a cyberattack, make the goal of minimizing both information ambiguity very difficult with the tools available. The findings, training applications, and user interface improvements made through serious games, gamification research, and cyber ranges have the potential to greatly decrease fog of war while increasing operational readiness and efficacy in cyber defence space [34].

6.5.2 Impact of Training in Digital Forensics

Digital forensics is necessary for law enforcement and investigation but also has applications in commercial, private, or institutional organizations. All activity conducted on an individual's computer systems and on a company network leaves a digital trace, which can range from web browser history caches and cookies all the way to document metadata, deleted file fragments, email headers, process logs, and backup files [37]. With cyber ranges, trainees learn to dissect and analyse real forensic cases. During such specific training, not only the technical aspects of digital forensics are considered but also the legal and organizational aspects.

The main purpose of the digital forensics' simulation environment is the ability to compile detailed forensic reports by trainees for use in both organization and in a court of law. A hands-on lab with basic forensics process and methodology scenarios demonstrates the ability to use forensics tools and analyse artefacts such as Windows file systems, Windows registry, memory images, Windows logs, and (optionally) network packet captures. This lab has frequently complicated configurations of multiple

computers networked to each other, to a common server, to network devices, or a combination of these. Securing a scene and collecting digital evidence in these environments may pose challenges to the first responder. Improperly shutting down a system may result in lost data, lost evidence, and potential civil liability. The first responder may find a similar environment to train and learn in safe similar locations, in order to be ready to deal with real case scenarios. These kinds of environments need to be built according to true needs and expectations along with the proper standards. The main objective of digital forensics training in a cyber range is to present the trainees with the principles of digital forensics and evidence gathering. Furthermore, there is an intention to establish a common knowledge of the requirements regarding evidence admissibility in the court of law along with the server-centric approach to evidence gathering as a valuable source for further legal proceedings as well as for establishing patterns of malicious activity. The patterns are then used to quickly identify similar events from the past in the future as they take place. A CR digital forensics exercise also gives an overview of popular malware characteristics, methods of identification, and tools that may be used at the real scene especially in a situation where the case is supported by LEAs.

Law enforcement agencies perform an essential role in achieving our nation's cybersecurity objectives by investigating a wide range of cybercrimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. It is important to develop and execute a cyber range training plan to maximize the readiness to conduct high-impact criminal investigations and disrupt/defeat cybercriminals. The added value is to prioritize the training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools through cyber range training. Criminal investigators and network security experts should be trained for a deeper understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting with updated and well-designed scenarios. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace.

6.6 FORESIGHT Paradigm

The EU H2020 FORESIGHT project aims to develop a federated cyber range solution in order to enhance the preparedness (prevention, detection, reaction, and mitigation) of cybersecurity professionals at all levels

(from junior to senior) by delivering a realistic training and simulation platform that brings together unique cybersecurity aspects from the aviation, power grid, and naval ecosystems. Hybrid scenarios will also be implemented by introducing IoT-simulated devices (e.g. sensors) to the ecosystems. FORESIGHT proposes the development and deployment of a beyond the state-of-the-art federated cyber-training environment, able to cater for multi-domain cyber training scenarios. To realistically and practically achieve this task, FORESIGHT proposes the design, development, and deployment of an internetworked federated controller that will provide gateway functionality between the multi-domain cyber ranges and will also provide virtual machines management and deployment capabilities. In this respect, FORESIGHT will enable the creation of a large-scale federated cyber range environment that can deliver multi-domain cyber training scenarios. Such kind of hybrid scenarios will include sub-scenarios across a range of domains (aviation, smart power grid, naval, or similar). In order to develop such scenarios to "feed" cyber range, current approaches and standards shall be considered in order to specify the best practices to be followed, improvements that are to be made, and constraints that are to be met, concurrently avoiding traps and obstacle that were faced in past implementations. The main driver of the system architecture will be the user requirements, ensuring that the system to be implemented meets the user needs and is able to provide the capabilities required. End-users from the above-mentioned domains replicate and configure critical systems of the airport/power grid/ports on the cyber range modelling and replicate IT and OT networks in order to build a near-real environment through a cyber range. The training will improve its cyber defence strategy and train its cybersecurity teams.

6.7 Conclusions

Cybersecurity training is growing in an appropriate way that is able to prevent and handle cyber breaches. New strategic methods such as anomaly detection, threat intelligence, simulation tools, big data analysis, threat analysis, forensic evidence collection, and gamification are needed in order to provide sufficient situational awareness of cybersecurity threats to companies, governments, and researchers. Cyber ranges can provide a continuous training environment using state-of-the-art methodologies, techniques, and a multi-domain training program directly guiding cybersecurity experts and professionals to create ways to implement and

integrate security measures. In respect to the above, this chapter gives a well-defined overview of the existing cyber ranges, focusing specifically on LEAs and defence stakeholders. Finally, the FORESIGHT approach has been described giving a projection of the future capabilities and potentials about cyber ranges design, implementation, and execution of training which target the involvement of the end-users.

Acknowledgements The FORESIGHT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833673. The results reflect only the author's view, and the agency is not responsible for any use that may be made of the information it contains.

References

1. DoD CR [Online]. Available: https://www.hqmc.marines.mil/docscr/. Accessed 27 Nov 2019.
2. Arizona Cyber Warfare Range [Online]. Available: https://www.azcwr.org/. Accessed 27 Nov 2019.
3. HNS platform [Online]. Available: https://www.hns-platform.com/. Accessed 27 Nov 2019.
4. ManTech [Online]. Available: https://www.mantech.com/capabilities/cyber. Accessed 27 Nov 2019.
5. École Navale CR [Online]. Available: https://www.chaire-cyber-navale.fr/. Accessed 27 Nov 2019.
6. AirBus CR [Online]. Available: https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/. Accessed 27 Nov 2019.
7. Kypo CR [Online]. Available: https://www.kypo.cz/en. Accessed 27 Nov 2019.
8. Augusta Cyber Range [Online]. Available: https://cyber.augusta.edu/georgia/. Accessed 27 Nov 2019.
9. US Cyber Range [Online]. Available: https://www.uscyberrange.org/. Accessed 27 Nov 2019.
10. AIT [Online]. Available: https://www.ait.ac.at/en/research-topics/cyber-security/cyber-range/. Accessed 27 Nov 2019.
11. Saros [Online]. Available: http://www.saros.co.uk/products/it/cyber-range/. Accessed 27 Nov 2019.
12. Rhea CR [Online]. Available: https://www.rheagroup.com/services/cyber-and-physical-security. Accessed 27 Nov 2019.
13. Virginia CR [Online]. Available: https://www.virginiacyberrange.org/. Accessed 27 Nov 2019.

14. The Michigan CR [Online]. Available: https://www.merit.edu/cyberrange/. Accessed 27 Nov 2019.
15. Ixia CR [Online]. Available: https://www.ixiacom.com/solutions/cyber-range. Accessed 27 Nov 2019.
16. Palo Alto [Online]. Available: https://www.paloaltonetworks.com/solutions/initiatives/cyberrange-overview. Accessed 27 Nov 2019.
17. IBM [Online]. Available: https://www.ibm.com/security/services/managed-security-services/security-operations-centers. Accessed 27 Nov 2019.
18. Cybexer [Online]. Available: https://cybexer.com/. Accessed 27 Nov 2019.
19. Raytheon [Online]. Available: https://www.raytheon.com. Accessed 27 Nov 2019.
20. Cyberbit [Online]. Available: https://www.cyberbit.com/solutions/cyber-range/. Accessed 27 Nov 2019.
21. Breaking Point [Online]. Available: https://www.ixiacom.com/products/network-security-testing-breakingpoint. Accessed 27 Nov 2019.
22. RGCE [Online]. Available: https://jyvsectec.fi/cyber-range/. Accessed 27 Nov 2019.
23. Berkatweb [Online]. Available: https://www.berkatweb.com/cyber-range/. Accessed 27 Nov 2019.
24. Cyber-Gym [Online]. Available: https://www.cybergym.com/. Accessed 27 Nov 2019.
25. Cisco Threats Report [Online]. Available: https://www.cisco.com/c/en/us/products/security/security-reports.html. Accessed 03 Dec 2019.
26. Cyber-security training: A comparative analysis of cyber ranges and emerging trends [Online]. Available: https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/2864976/theFile. Accessed 02 Dec 2019.
27. CyberCents [Online]. Available: https://cybercents.com/cyber-ranges/cents/. Accessed 27 Nov 2019.
28. Silensec Cyber Range [Online]. Available: https://cyberranges.com/#cyber-range-securing-cyber-space. Accessed 27 Nov 2019.
29. [MISP – Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing [Online]. Available: http://www.misp-project.org. Accessed 02 Dec 2019.
30. Lessons learned from complex hands-on defense exercises in a cyber range [Online]. Available: https://ieeexplore.ieee.org/document/8190713. Accessed 02 Dec 2019.
31. Locked Shields 2018 After Action Report. Accessed 02 Dec 2019.
32. NIST: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities [Online]. Available: https://www.nist.gov/publications/guide-test-training-and-exercise-programs-it-plans-and-capabilities. Accessed 04 Dec 2019.

33. Smith, R. (2010). The long history of gaming in military training. *Simulation and Gaming, 41*, 6–19. https://doi.org/10.1177/1046878109334330.
34. CSS Cyber Defense Report, Cybersecurity and Cyber defense Exercises [Online]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf. Accessed 04 Dec 2019.
35. Prior, T., & Roth, F. (2016). *CSS study: Learning from disaster events and exercises in civil protection organizations (CSS Study), risk and resilience reports.* Zurich: Center for Security Studies.
36. CCDCOE Cyber Defense Exercise [Online]. Available: https://ccdcoe.org/exercises/locked-shields/. Accessed 04 Dec 2019.
37. Role and impact of digital Forensics in cyber crime investigations [Online]. Available: https://www.researchgate.net/publiction/331991596_ROLE_AND_IMPACT_OF_DIGITAL_FORENSICS_IN_CYBER_CRIME_INVESTIGATIONS/link/5c9a39c445851506d72d8fdc/download. Accessed 04 Dec 2019.
38. Qiu, P., Cisco Cyber Range [Online]. Available: https://www.cisco.com/c/dam/global/en_hk/assets/event/cisco_connect_2015/pdf/4-3.pdf. Accessed 17 Dec 2019.